A Maintenance System based on Near Field Communication

Stephan Karpischek, Florian Michahelles, Albrecht Bereuter, Elgar Fleisch
Department of Management, Technology and Economics
ETH Zurich, Switzerland
{skarpischek, fmichahelles, abereuter, efleisch}@ethz.ch

Abstract

Maintenance of critical emergency infrastructure is potentially lifesaving, but also expensive and tedious to document and track. In this paper we demonstrate a maintenance system based on Near Field Communication (NFC). NFC-enabled mobile phones and NFC tags are used to improve recurring maintenance processes: the maintenance task itself becomes more efficient; and the system facilitates real-time documentation, central process control, and proof of site presence.

1. Introduction

Maintenance of critical emergency infrastructure is a potentially lifesaving activity. Therefore, a proactive maintenance strategy with strict maintenance intervals and accurate documentation is necessary and often prescribed by safety and security regulations [1]. Unfortunately, maintenance tasks are mostly perceived as a "necessary evil". They are time-consuming and unsatisfying for personnel [2]. With traditional paper-based methods, e.g., maintenance books, the proper fulfillment of maintenance tasks can only be controlled in a very limited way. It is easy to falsely claim fulfillment of maintenance tasks, e.g., by simply filling out maintenance books once in a while or just before control. As such false claims are relatively hard to discover, there is only little risk for the personnel. Compared to this, the overall risk of poor or missing maintenance of these facilities can be rather high [3].

This paper demonstrates an NFC-based system which makes false claims harder, using a server-based process control and documentation web site and synchronized secrets for an improved proof of site presence. Our demonstrator implements weekly maintenance of sprinkler systems, a task which is required by legal regulations for fire sprinkler systems installed in Switzerland. The maintenance task consists of controlling pressure meters, valves, etc. Figure 1 shows valves and meters of a typical sprinkler system whose proper function needs to be checked weekly.

Figure 1: Fire sprinkler system

2. Related Work

Maintenance systems based on Radio Frequency Identification (RFID) already exist, e.g., for airports and have increased efficiency and security of maintenance processes there [1]. However, these systems use industrial mobile RFID readers and are therefore rather expensive to implement.

The main use of NFC is in the area of payment [4] and ticketing, but also more generally for mobile interaction [5]. Previous user studies have shown that NFC is a very intuitive and convenient way to identify tagged objects [6,7].

Some companies, e.g., Adamsoft [14] or Over-C are already offering NFC-based solutions to document

presence of personnel at checkpoints for guarding houses and facilities.

3. Concept

Our goal is to improve the quality of recurring maintenance tasks. We propose to use NFC-enabled mobile phones for this. Collected data like pressure values or correct position of the valves can be entered directly on the mobile phone. The presence of the maintenance personnel at the point of maintenance is enforced by physically attaching NFC tags to the checkpoints and by making touching the NFC tags with the mobile phone an obligatory part of the process. This is done by applying synchronized secrets, a method also used against counterfeiting to the area of maintenance. In the following subsections we give an overview over the system's design, present the method of synchronized secrets, and describe the maintenance process with the proposed NFC-based system.

3.1. System design

The system consists of a client application on the NFC-enabled mobile phone which we called “Facility Manager”; re-writable NFC tags which are attached to or near the checkpoints; and a central server application connected to a database for storing maintenance information. Communication between the mobile client and the server uses web services.

We use low cost tags and NFC-enabled mobile phones. In contrast to other services that rely only on reading object's tags, the proposed system needs to write random data to the tags to provide a higher level of security. During the actual maintenance task, the system does not rely on an available Internet connection. Only a temporary Internet connection is needed at some time before and after the actual maintenance task to synchronize data between the mobile client and the server. Thus, the system can also be used with offline data entry and inside facilities with little or no network coverage.

The server system can either be run by the facility owner or by an external company, e.g., facility management company, insurance company, or federal authority. In any case, central and real-time documentation and control of the maintenance process is possible. The documentation of the maintenance process is available online on a website immediately after the maintenance task is fulfilled and the maintenance data uploaded.

The server system can also be used to send automated reminders to the facility maintenance personnel via E-Mail or text messages. If a maintenance cycle is missed these communication channels can be used to notify authorities or trigger alarms.

3.2. Synchronized secrets

Touching the checkpoint tags – and thus presence at the point of maintenance – is enforced by using synchronized secrets. This method has been proposed earlier for use with RFID tags for detection of cloned RFID tags, i.e. counterfeit products, in supply chains [8,9]. Here, synchronized secrets are used with NFC tags to proof the physical presence of personnel at the checkpoint. A sequence of random bytes (secret) is generated in the server application for every checkpoint at the beginning of every week. When the maintenance process is started, the client application downloads the secrets of the current week from the server. During the actual maintenance task the secrets are written to the corresponding NFC tags. In the next maintenance cycle the secrets are read from the NFC tags, compared with the stored ones of the previous cycle on the server, and again updated by new random bytes.

Missing maintenance cycles are easily detected as outdated synchronized secrets and immediately visible on the server website. As the maintenance personnel needs to write the current secret to the checkpoint's NFC tag every time and transfer the maintenance data to the server, it is not possible to falsely claim having been at the checkpoint (non-repudiation). Either, the maintenance cycle would be marked as missed on the documentation and control website, or the secrets on the checkpoint's tags would differ from the secrets on the server. This would trigger a mismatch at the next maintenance cycle and can also be easily detected by a controlling party comparing the stored secrets at the checkpoints with the current secrets on the server.

3.3. Process description

When the system is installed, NDEF messages with input field records and initial secrets are written to NFC tags. These tags are securely attached to the checkpoints of the fire sprinkler system. The maintenance personnel is equipped with NFC-enabled mobile phones with the Facility Manager application

Figure 2: Screens of the mobile phone client application Facility Manager

pre-installed. On the server application a new instance is created.

The weekly maintenance process consists of three steps:

Step 1: The user starts the NFC Facility Manager client application on the NFC-enabled mobile phone and is then asked to start the maintenance process. The client application opens an Internet connection and downloads the secrets for the current week from the server application. The mobile phone's unique identifier is used to authenticate the device. The Internet connection is closed again and the user is asked to touch a checkpoint at the point of maintenance. The number of total checkpoints needed is shown on the mobile phone display.

Step 2: When touching the NFC tag of a checkpoint, the client application reads the unique tag ID, the stored secret, the label of the checkpoint and the type of input required from the NFC tag. It then writes the new corresponding secret to the checkpoint's tag. Then, an input field is displayed on the mobile phone screen for data entry. The input value is stored together with the tag ID, the read secret and a timestamp in the mobile phone. This step is repeated for every checkpoint until all checkpoints are done. No Internet connection is needed for this.

Step 3: When all checkpoints are done, the user is asked to finish the maintenance process. The application then opens a new Internet connection and uploads the collected data to the server application. On the server website the task for this week is now marked as done.

4. Implementation

The maintenance checkpoints are tagged with rewritable NFC Forum Tag Type 1 tags with a storage size of 1kbit [11]. The tags store an NFC Data Exchange Format (NDEF) message with two records [12]. We introduce a new external record type – the input field record – and use the URN "urn:nfc:ext:ethz.ch:if" to identify this record type [10]. The record contains two fields: Text for a label and the type of the input field, which is stored as an integer value. For the demonstrator, two different types of input field are used: A text field (identified by the value 0) and a boolean choice group (1). More input field types would be possible corresponding to the various input field types offered by the J2ME user interface abstraction. Currently, the text field type is used for input of, e.g., pressure values, and the boolean choice group is used for answering yes/no questions. The secret is stored in an additional text record.

The mobile client application is implemented as a J2ME midlet on a Nokia 6212 classic mobile phone. We used the Series 40 Nokia 6212 NFC SDK for development [13].

The server application is implemented with the web application framework Ruby on Rails. A sqlite database is used for storing and archiving the maintenance information. Communication between the client and the server uses web services over HTTP, using the concepts of ReST and JSON as the data exchange format. The control screen can be accessed with any web browser.

Figure 2 shows some screens of the mobile client application. Figure 3 shows the screen of the documentation and control website. Figure 4 shows the client application in use at the point of maintenance.

5. Discussion

Compared to existing paper-based processes, the proposed system brings several advantages:

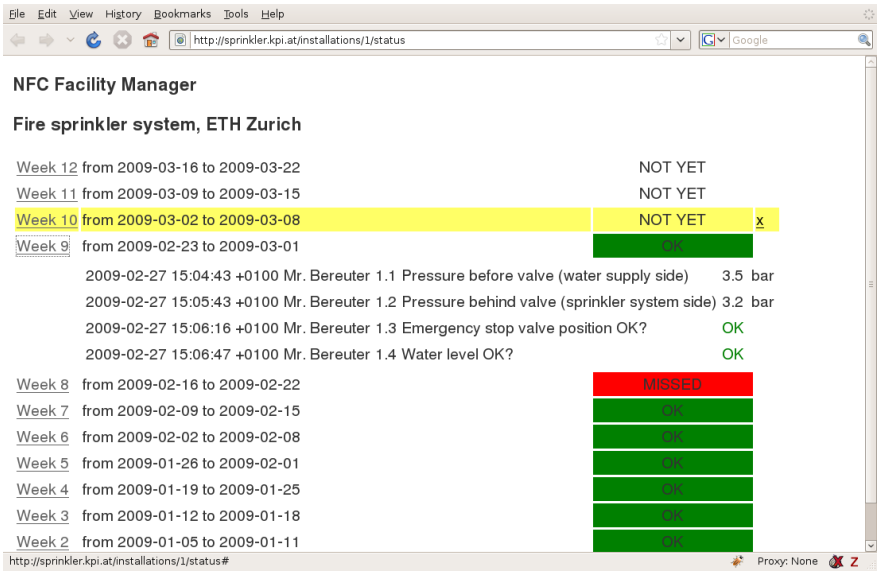

Figure 3: Documentation and control website

Figure 4: Use of the client application

The mobile input of maintenance data and transfer to a central database allows for online and real-time documentation on a website. Thus, proper and timely fulfillment of the maintenance task can be easily controlled in one central place. The server can also be used to send automated reminders or to notify authorities in case of missed maintenance.

Mobile phone devices are perceived as a very personal device and can be uniquely identified. Thus, maintenance personnel can be authenticated with the system. Object identification with NFC is perceived as fast, reliable and intuitive. The method of synchronized secrets makes false claims of task fulfillment very difficult. Compared to solutions with other mobile RFID readers, the implementation of an NFC-based system is relatively cheap.

A first evaluation was done by presenting our solution to a group of risk engineers of leading industry insurance companies, where we received very positive feedback and great interest. The solution was also presented to management executives of fire sprinkler system providers who considered the solution well suited for medium sized installations. According to them larger sprinkler systems are already connected to enterprise information systems.

6. Conclusion

This work presented an NFC-based system for recurring maintenance processes. It combines the ease of use of NFC with central process control and documentation. For implementation we introduced a new NDEF record type for input fields and applied the method of synchronized secrets for proofing the presence of maintenance personnel at the point of maintenance. In our opinion the proposed system offers significant benefits over traditional approaches for facility maintenance. Its implementation is relatively cheap compared to other solutions. Future work will include further evaluation of the system in user studies

and on-site trials together with facility management and insurance companies.

References

[1] C. Legner and F. Thiesse, "RFID-based Maintenance at Frankfurt Airport", *IEEE Pervasive Computing*, Jan.-Mar. 2006, pp. 34-39.

[2] D. Sherwin, "A review of overall models for maintenance management", *Journal of Quality in Maintenance Engineering,* Vol. 6, no. 3, Sept. 2000, pp. 38-164.

[3] V. Narayan, "The raison d'être of maintenance", *Journal of Quality in Maintenance Engineering,* Vol. 4, no. 1, 1998, pp. 38-50.

[4] J. Ondrus, Y. Pigneur, "An Assessment of NFC for Future Mobile Payment Systems", International Conference on Mobile Business (ICMB'07), Jul. 2007, Toronto, Canada.

[5] O. Falke, E. Rukzio, U. Dietz1, P. Holleis, A. Schmidt, "Mobile Services for Near Field Communication", Technical Report LMU-MI-2007-1, ISSN 1862-5207. Munich, Germany. March 2007.

[6] A. Geven, P. Strassl, B. Ferro, M. Tscheligi, and H. Schwab, "Experiencing real-world interaction: results from a NFC user experience field trial," Proceedings of the 9th international conference on Human computer interaction with mobile devices and services, Singapore: ACM, 2007, pp. 234-237.

[7] E. Rukzio, G. Broll, K. Leichtenstern, A. Schmidt, "Mobile Interaction with the Real World: An Evaluation and Comparison of Physical Mobile Interaction Techniques.", European Conference on Ambient Intelligence (AmI-07). Darmstadt, Germany. 7-10 November 2007.

[8] M. Lehtonen, D. Ostojic, A. Ilic, F. Michahelles, "Securing RFID systems by detecting tag cloning", *The Seventh International Conference on Pervasive Computing*, Pervasive'09, Japan, May 2009.

[9] A. Ilic, M. Lehtonen, F. Michahelles, E. Fleisch, "Synchronized Secrets Approach for RFID-enabled Anti-Counterfeiting", Demo at Internet of Things Conference 2008, Zurich, Switzerland, 2008.

[10] NFC Forum, "NFC Record Type Definition (RTD) Technical Specification", 2006. Available: http://www.nfc-forum.org/.

[11] NFC Forum, "NFC Forum Type 1 Tag Operation Specification", 2007. Available: http://www.nfc-forum.org/.

[12] NFC Forum, "NFC Data Exchange Format (NDEF)", 2006. Available: http://www.nfc-forum.org/ .

[13] Series 40 Nokia 6212 NFC SDK. Available: http://www.forum.nokia.com/ .

[14] "NFC Guard Tour Verification", Available: http://www.adamsoft.com/nfc/NFCGuardTourVerification.pdf .